REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is made obvious under the provisions of 35 U.S.C. § 103. Thus, the Applicants believe that all of these claims are now in allowable form.

I. OBJECTION TO THE SPECIFICATION

The specification stands objected to for informalities. In response, the Applicants have amended the specification in order to address these informalities.

In particular, the paragraph beginning on page 9, line 18 and ending on page 9, line 26 has been amended to provide the serial number of the referenced United States patent application, and the paragraph beginning on page 11, line 14 and ending on page 12, line 4 has been amended to remove the embedded hyperlinks.

Accordingly, the Applicants respectfully request that the objection to the specification be withdrawn.

II. REJECTION OF CLAIMS 1-6, 8-23, 25-40 AND 42-51 UNDER 35 U.S.C. § 103

Claims 1-6, 8-23, 25-40 and 42-51 stand rejected as being unpatentable over the Bots et al. patent (United States Patent No. 6,226,748, issued May 1, 2001, hereinafter "Bots") in view of the Pandya et al. patent (United States Patent No. 6,671,724, issued December 30, 2003, hereinafter "Pandya"). The Applicants respectfully traverse the rejection.

Particularly, the Examiner's attention is directed to the fact that Bots fails to disclose or suggest the novel invention of a virtual private network (VPN) in which master nodes control admission and departure in the VPN for an associated non-empty subset of member nodes, as well as facilitate VPN communications between the member nodes, and in which all communications between the nodes are encrypted, as claimed in Applicants' independent claims 1, 18 and 35.

In contrast, Bots at most teaches a security device (*i.e.*, a VPN unit or VPNU) that performs encryption or decryption on intercepted communications en-route between member nodes of VPNs. That is, as described by the cited passage of Bots

(*i.e.*, column 6, lines 37-52), the VPNU associated with a sender "will process the data packet from the sending side in such as way as to ensure that it [is] encrypted, authenticated and optionally compressed" (emphasis added). The VPNU associated with the receiver handles "the process of decrypting and authenticating the packets before forwarding it toward the destination endstation" (emphasis added). Thus, communications are encrypted as they travel between VPNUs, but not encrypted as they travel to/from nodes (*i.e.*, the sending node and the receiving node).

FIG. 2 of Bots (attached and annotated herewith as Appendix I) clearly illustrates this point. For example, if sender 202 of LAN 205 wishes to send a data packet to remote receiver 331 of LAN 235, the packet would "initially be treated as an ordinary Internet data packet transfer" (*See*, Bots, column 6, lines 58-59, emphasis added) until it reaches the sender's associated VPNU 250. At the VPNU 250, the data packet is processed "undergoing various combinations of compression, encryption and authentication" (*See*, Bots, column 7, lines 23-24) and then forwarded over the Internet 250 to the VPNU 256 associated with the receiver 331. The receiving VPNU 250 "reverses the [compression, encryption and authentication] processes" (*i.e.*, decrypts the packet) and then delivers the packet to the receiver 331 (*See*, Bots, column 7, lines 56-57). Thus, again between the receiving VPNU 250 and the receiver 331, the packet is again treated as an ordinary Internet data packet transfer. Clearly, then, the only point at which the packet is encrypted is when it travels from the sending VPNU 250 to the receiving VPNU 256. The packet is not encrypted when it is sent by the sender 202, or received by the receiver 331. Thus, communications between nodes are not encrypted.

Compare this to, for example, Applicants' FIG. 2 (attached and annotated herewith as Appendix II). If sender 220a wishes to send a data packet to receiver 220b, the sender 220a encrypts the packet, in accordance with an encryption key distributed by the master node 210, before sending the packet. Likewise, the receiver 220b decrypts the received packet in accordance with the encryption key. Thus, the communication between the nodes (*i.e.*, the sender and the receiver) is encrypted, as both nodes directly participate in the encryption/decryption process. There is no need

for an intermediary, such as the VPNU of Bots, to perform encryption/decryption on intercepted packets.

Notably, Applicants' invention positively claims master nodes that control admission and departure in a VPN for an associated non-empty subset of member nodes, as well as facilitate VPN communications between the member nodes, and in which all communications between the nodes are encrypted, as claimed in Applicants' independent claims 1, 18 and 35. Specifically, Applicants' claims 1, 18 and 35 positively recite:

1. A group management system comprising:
a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted; and
a plurality of master nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes and further facilitating said communications between said plurality of interconnected nodes, wherein in the event one of the master nodes fails, the associated subset of member nodes will be automatically reassigned to one or more other of the master nodes. (Emphasis added)

18. A method for managing a group, the method comprising:
providing a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted; and
providing a plurality of master nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes and further facilitating said communications between said plurality of interconnected nodes, wherein in the event one of the master nodes fails, the associated subset of member nodes will be automatically reassigned to one or more other of the master nodes. (Emphasis added)

35. A computer readable medium containing an executable program for managing a group, where the program performs the steps of:
providing a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"), wherein all communications between said interconnected nodes are encrypted; and
providing a plurality of master nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member

nodes and further facilitating said communications between said plurality of interconnected nodes, wherein in the event one of the master nodes fails, the associated subset of member nodes will be automatically reassigned to one or more other of the master nodes. (Emphasis added)

The Applicants' invention is directed to systems and methods for scalable distributed management of virtual private networks (VPNs). The management of encrypted group communications necessary to establish secure, private VPN communications channels through an underlying public network infrastructure places a variety of burdens on a VPN manager. In particular, the addition or removal of a member from a VPN often involves the generation and distribution of one or more new encryption keys that allow current VPN members to decrypt private communications sent through the VPN, but prevent non-VPN members from decrypting the communications. As VPN membership increases and changes dynamically with greater frequency, the complexity of encryption key management becomes even more burdensome. Thus, the VPN manager becomes a single point of failure for the entire VPN; overload of the VPN manager can cause the entire VPN to fail. This makes the VPN architecture very difficult and very costly to scale, which is not ideal for enterprises relying on secure and private electronic communications.

The Applicants' invention enhances the scalability of a VPN by dividing the member nodes of the VPN, which communicate with each other via encrypted communications, into subsets and providing a plurality of master nodes that are each associated with a subset of member nodes to control membership (*i.e.*, admission and departure) in the VPN and to facilitate VPN communications for that subset. For example, each master node is responsible for managing the generation and distribution of encryption keys for only its associated subset(s), so that VPN communication and management burdens are not placed entirely on a single master node. This eliminates the single point of failure, because if one master node fails, any one of a plurality of other master nodes is available to assume the failed node's responsibilities. Moreover, the member nodes are able to use the distributed encryption keys to communicate directly with each other using encrypted communications. Thus, a VPN employing such an architecture is more easily scalable than a VPN employing a more conventional

architecture, because a plurality of new member nodes may be added or admitted to the VPN through a discrete master node.

The Applicants' invention positively claims that communications between nodes are encrypted. That is, in at least claims 1, 18 and 35, the Applicants recite the limitation of encrypted communications between member nodes of a VPN. As described above, Bots does not teach or suggest a mechanism for allowing direct, encrypted communications between nodes, but rather teaches a communication intercept point that encrypts or decrypts messages seen by the nodes as ordinary Internet data packet transfers.

Bots thus fails to teach or anticipate a virtual private network (VPN) in which master nodes control admission and departure in the VPN for an associated non-empty subset of member nodes, as well as facilitate VPN communications between the member nodes, and in which all communications between the nodes are encrypted, as positively claimed by the Applicants in claims 1, 18 and 35. Pandya fails to bridge this gap in the teachings of Bots. Therefore, for at least the reasons set forth above, the Applicants submit that independent claims 1, 18 and 35 fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Dependent claims 2-6, 8-17, 19-23, 25-34, 36-40 and 42-51 depend from claims 1, 18 and 35 and recite additional features therefore. As such, and for at least the reasons set forth above, the Applicants submit that claims 2-6, 8-17, 19-23, 25-34, 36-40 and 42-51 are not made obvious by the teachings of Bots in view of Pandya. Therefore, the Applicants submit that dependent claims 2-6, 8-17, 19-23, 25-34, 36-40 and 42-51 also fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

III. INFORMATION DISCLOSURE STATEMENT

The Applicants are filing herewith an information disclosure statement citing several United States patents. The Examiner is respectfully encouraged to review the cited references in connection with any response to this communication.

IV. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §103. Consequently, the Applicants believe that all of the presented claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

7/20/06
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702